About Us:

**Wesley Tanner**
- Systems Engineer for a Software-Defined Radio (SDRF) company
- B.S. Electrical Engineering from RPI

**Nick Lane-Smith**
- Security Engineer for a computer company in Cupertino...
- B.S. Computer Science from UCSB

**Keith Lareau** (not present)
- B.S. Computer Science and Computer Systems Engineering from RPI

CellularCrypto.com
Presentation Overview

• Motivation, the need for Cellular Crypto
• Current market offerings
  – Operational details
• A new approach - GSM Voice Channel Modem
  – Details of the voice channel
  – Radio interface
  – Traditional PSTN modems over GSM
• Cryptographic Design
• Demonstrations

CellularCrypto.com
Motivation

Where is End-to-End voice protection over cellular?

Why hasn’t it become a reality for the average consumer?
GSM Overview

Structure of a GSM network (key elements)

- Base Station Subsystem (BSS)
  - BTS
  - Air (Um)
  - A-bis

- MSC / VLR
  - H/E etc
  - SS7 Network

- Network SubSystem (NSS)
  - HLR
  - AUC (EIR)

- GPRS Core Network
  - SGSN
  - GPRS backbone IP Network
  - GGSN
  - GPRS core network

- The Internet (or a corporate)

Interface Names
GSM Cryptography

A3 - Authentication algorithm for the GSM security model
A5 - The stream cipher used for voice-privacy
A8 - Algorithm for voice-privacy key generation.
A5 weaknesses

Alex Biryukov, Adi Shamir and David Wagner demonstrated breaking a A5/1 key in less than a second on a PC with 128 MB RAM.

Elad Barkhan, Eli Biham and Nathan Keller have shown a ciphertext-only attack against A5/2.
Moral of the story...

GSM Cryptography provides limited, if any, true security to your voice channel. Something additional is needed.
The NEED for Cellular Crypto

Cellular phones have almost completely supplanted PSTN.

Cellular companies do not provide ANY meaningful protection for voice traffic.

The ease of intercepting voice traffic is astounding...

And people do it all the time!
The NEED for Cellular Crypto

Two major classes of intercepts:

Government Perpetrated

- Authorized and Unauthorized
- Secret (FISA) and Reported
- Local, State and Federal
- Not just your own government

- Large portions of Telecom infrastructure in the USA are owned by Foreign corporations, supported by Foreign and possibly adversarial governments. (Israel, China, etc.)

CellularCrypto.com
The NEED for Cellular Crypto

Two major classes of intercepts:

Non-government Perpetrated

- Private Investigators
- Business Partners
- Economic Espionage
The **NEED** for Cellular Crypto

Government Intercept
- Probably the most common
- Undetectable:
  - They don’t waste time intercepting wireless transmission. CALEA Act allows to them execute intercept remotely via the telecom provider directly.
- "Untraceable" prepaid/disposable is no protection if you exhibit same calling pattern
- Presumably highest level (NRO, NSA ...) can perform voice match as well
The **NEED** for Cellular Crypto

Let’s look at the data for reported intercepts

In 2004:

1,710 Authorized intercepts
1,507 Targeted “Portable device” (Cellular)
The **NEED** for Cellular Crypto

From U.S. Courts 2004 Wiretap Report:

Table 7

Authorized Intercepts Granted Pursuant to 18 U.S.C. 2519 as Reported in Wiretap Reports for Calendar Years 1994 - 2004

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept applications requested</td>
<td>1,154</td>
<td>1,058</td>
<td>1,150</td>
<td>1,186</td>
<td>1,331</td>
<td>1,350</td>
<td>1,190</td>
<td>1,491</td>
<td>1,359</td>
<td>1,442</td>
<td>1,710</td>
</tr>
<tr>
<td>Intercept applications authorized</td>
<td>1,154</td>
<td>1,058</td>
<td>1,149</td>
<td>1,186</td>
<td>1,329</td>
<td>1,350</td>
<td>1,190</td>
<td>1,491</td>
<td>1,358</td>
<td>1,442</td>
<td>1,710</td>
</tr>
<tr>
<td>Federal</td>
<td>554</td>
<td>532</td>
<td>581</td>
<td>569</td>
<td>566</td>
<td>601</td>
<td>479</td>
<td>486</td>
<td>497</td>
<td>578</td>
<td>730</td>
</tr>
<tr>
<td>State</td>
<td>600</td>
<td>526</td>
<td>568</td>
<td>617</td>
<td>763</td>
<td>749</td>
<td>711</td>
<td>1,005</td>
<td>861</td>
<td>864</td>
<td>980</td>
</tr>
<tr>
<td>Avg. days of original authorization</td>
<td>29</td>
<td>29</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>27</td>
<td>28</td>
<td>27</td>
<td>29</td>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>Number of extensions</td>
<td>861</td>
<td>834</td>
<td>887</td>
<td>1,028</td>
<td>1,164</td>
<td>1,367</td>
<td>926</td>
<td>1,008</td>
<td>889</td>
<td>1,145</td>
<td>1,341</td>
</tr>
<tr>
<td>Average length of extensions (in days)</td>
<td>29</td>
<td>29</td>
<td>28</td>
<td>28</td>
<td>27</td>
<td>29</td>
<td>28</td>
<td>29</td>
<td>29</td>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>Location of authorized intercepts:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Residence</td>
<td>451</td>
<td>428</td>
<td>434</td>
<td>382</td>
<td>436</td>
<td>341</td>
<td>244</td>
<td>206</td>
<td>154</td>
<td>118</td>
<td>83</td>
</tr>
<tr>
<td>Business</td>
<td>118</td>
<td>101</td>
<td>101</td>
<td>78</td>
<td>87</td>
<td>59</td>
<td>56</td>
<td>60</td>
<td>37</td>
<td>35</td>
<td>30</td>
</tr>
<tr>
<td>Portable device</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>719</td>
<td>1,007</td>
<td>1,046</td>
<td>1,165</td>
</tr>
<tr>
<td>Multiple locations</td>
<td>97</td>
<td>115</td>
<td>149</td>
<td>197</td>
<td>222</td>
<td>287</td>
<td>109</td>
<td>117</td>
<td>85</td>
<td>95</td>
<td>65</td>
</tr>
<tr>
<td>Not indicated or other*</td>
<td>488</td>
<td>414</td>
<td>465</td>
<td>529</td>
<td>584</td>
<td>663</td>
<td>62</td>
<td>101</td>
<td>36</td>
<td>29</td>
<td>25</td>
</tr>
</tbody>
</table>
The NEED for Cellular Crypto

Cellular intercepts have doubled since 2000, the trend appears to suggest that the ease of intercepts is the reason behind growth.

Of note, there is no jump after Sept. 11th, which implies FISA intercepts are used for intercepts relating to terrorism. The overall number of intercepts is most likely orders of magnitude greater.
The **NEED** for Cellular Crypto

- GSM Spec TS 33.106
- Interception function should not alter the target’s service or provide indication to any party involved.
- Output ‘Product’ and/or ‘Network related data’
- Network related data - location, type of call, all party’s numbers.
- Product - speech, user data, fax or SMS.
Diagram of a Lawful Intercept
Moral of the story...2

Even if the GSM crypto sufficiently protected the handset->tower, network transit layers are capable of being intercepted.

Only End-to-End crypto can provide sufficient security.
Current Market Offerings

Various GSM Crypto products:

– Cryptophone G10
– Sectera by General Dynamics (govt. contract)
– Ancort Crypto Smart Phone
– Several “vapor” products
Future Narrowband Digital Terminal

• FNBDT is a new US govt. standard for secure voice communication
• Needs minimum bandwidth of 2400 Hz.
• Replacement for STU-III
• Uses MELP for voice compression.
Problems with Current Products

They all use the GSM circuit switched data (CSD) channel

• This service is not part of the normal consumer-level package in all places.
• CSD is quickly being replaced by packet switched services, which do not have the necessary performance (currently) for a quality voice link.
• Long call setup times
• High latency, but not as bad as GPRS
Problems with Current Products

CSD is meant to carry data, not voice. Voice can tolerate more transmission errors and does not require ARQ.

High latency and retransmission rather than dropping a frame make data channel insufficient for voice.
Problems with Current Products

Some are only available for government or government contractor use, or are very expensive.

The solution needs to be available to everyone.
So, what then? Give up?

Wait for 3G? Will 3G even be sufficient?
Proposed Solution

Develop a modem that works over the GSM voice channel.
- Latency optimized
- Frame dropping

A fun and challenging technical problem to solve is a side benefit.
Technical Details of the GSM Voice Channel
The GSM Voice Channel

The voice channel has lots of useful properties

• Low latency
• High availability
• Friendly billing system from service providers. Use your standard voice minutes instead of possibly more expensive data packages.

However, the voice channel is forgiving only for speech-like waveforms.
### GSM Voice Channel Data Rate Calculation

<table>
<thead>
<tr>
<th>Description</th>
<th>Parameter</th>
<th>Parameter Number</th>
<th>Number of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Parameters</td>
<td>LAR 1</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>LAR 2</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>LAR 3</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>LAR 4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>LAR 5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>LAR 6</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>LAR 7</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>LAR 8</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>LTP Parameters</td>
<td>LTP Lag</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>LTP gain</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>RPE grid position</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Block amplitude</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 1</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 2</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 3</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 4</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 5</td>
<td>17</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 6</td>
<td>18</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 7</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 8</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 9</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 10</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 11</td>
<td>23</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 12</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 13</td>
<td>25</td>
<td>3</td>
</tr>
<tr>
<td>RPE Parameters</td>
<td>LTP Lag</td>
<td>26</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>LTP gain</td>
<td>27</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>RPE grid position</td>
<td>28</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Block amplitude</td>
<td>29</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 1</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 2</td>
<td>31</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 3</td>
<td>32</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 4</td>
<td>33</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 5</td>
<td>34</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 6</td>
<td>35</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 7</td>
<td>36</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 8</td>
<td>37</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 9</td>
<td>38</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 10</td>
<td>39</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 11</td>
<td>40</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 12</td>
<td>41</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 13</td>
<td>42</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Parameter</th>
<th>Parameter Number</th>
<th>Number of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTP Parameters</td>
<td>LTP Lag</td>
<td>43</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>LTP gain</td>
<td>44</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>RPE grid position</td>
<td>45</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Block amplitude</td>
<td>46</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 1</td>
<td>47</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 2</td>
<td>48</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 3</td>
<td>49</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 4</td>
<td>50</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 5</td>
<td>51</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 6</td>
<td>52</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 7</td>
<td>53</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 8</td>
<td>54</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 9</td>
<td>55</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 10</td>
<td>56</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 11</td>
<td>57</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 12</td>
<td>58</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 13</td>
<td>59</td>
<td>3</td>
</tr>
<tr>
<td>RPE Parameters</td>
<td>LTP Lag</td>
<td>60</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>LTP gain</td>
<td>61</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>RPE grid position</td>
<td>62</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Block amplitude</td>
<td>63</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 1</td>
<td>64</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 2</td>
<td>65</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 3</td>
<td>66</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 4</td>
<td>67</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 5</td>
<td>68</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 6</td>
<td>69</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 7</td>
<td>70</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 8</td>
<td>71</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 9</td>
<td>72</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 10</td>
<td>73</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 11</td>
<td>74</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 12</td>
<td>75</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>RPE pulse 13</td>
<td>76</td>
<td>3</td>
</tr>
</tbody>
</table>

**Total Bits: 260**  
**Frame rate (fps): 50**  
**Data rate (kbps): 13**
# Full Rate Channel Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bits per frame</td>
<td>2080</td>
<td>260</td>
</tr>
<tr>
<td>frames per second</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>data rate (kbps)</td>
<td>104000</td>
<td>13000</td>
</tr>
<tr>
<td>Compression ratio</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>
Full Rate Channel Properties

- Regular Pulse Excitation - Long Term prediction - Linear Predictive Coder
- 260 bits per frame
- Bandwidth of 13 kbps
- Input is 160, 13 bit uniform quantized PCM samples
  - 8 kHz sampling rate
Encoder Block Diagram

Input signal → Pre-processing

Short term analysis filter

Short term LPC analysis

(1) Short term residual

Short term residual estimate (40 samples)

(2) Long term residual (40 samples)

(3) Short term residual estimate (40 samples)

LTP analysis

(4) Reconstructed short term residual (40 samples)

(5) Quantized long term residual (40 samples)

LTP parameters (9 bits/5 ms)

RPE grid selection and coding

RPE grid decoding and positioning

Reflection coefficients coded as Log. - Area Ratios
(36 bits/20 ms)

RPE parameters (47 bits/5 ms)

To radio subsystem
Reflection coefficients coded as Log. - Area Ratios (36 bits/20 ms)

RPE grid decoding and positioning

RPE parameters (47 bits/5 ms)

Short term synthesis filter

Post-processing

Output signal

Long term synthesis filter

LTP parameters (9 bits/5 ms)

From radio subsystem
Voice packet structure

• Some bits are protected for transmission over radio
  – Class A bits CRC protected
  – Class B/C bits sent uncoded
• Class A bits are most important for intelligible voice.
• RFC 3267
  – Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs
Properties of Speech
(as related to GSM full rate codec)

• Short term parameters
  – LPC

• Long term prediction, computed based on the output of the short term filtering
  – Lag
  – Gain

• Residual information
  – Calculated by the error in the estimated residual signal from the actual residual signal
Voice Samples - 8 kHz sample rate
Close-up Voice Samples
## Telephone Modem Modulation

<table>
<thead>
<tr>
<th>Name</th>
<th>Receive rate (bps)</th>
<th>Transmit rate (bps)</th>
<th>Symbol rate (baud)</th>
<th>Modulation Type</th>
<th>Transmit carrier frequencies (Hz)</th>
<th>Receive carrier frequencies (Hz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bell 103</td>
<td>300</td>
<td>300</td>
<td>300</td>
<td>FSK</td>
<td>1270/1070</td>
<td>2225/2025</td>
</tr>
<tr>
<td>CCITT V.22</td>
<td>1200</td>
<td>1200</td>
<td>600</td>
<td>DPSK</td>
<td>1200</td>
<td>2400</td>
</tr>
<tr>
<td>CCITT V.32</td>
<td>4800</td>
<td>4800</td>
<td>2400</td>
<td>QAM</td>
<td>1800</td>
<td>1800</td>
</tr>
<tr>
<td>ITU V.34</td>
<td>33600</td>
<td>33600</td>
<td>3429</td>
<td>TCM</td>
<td>1800</td>
<td>1800</td>
</tr>
<tr>
<td>ITU V.92</td>
<td>53000</td>
<td>48000</td>
<td>8000</td>
<td>PCM</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

CellularCrypto.com
56 kbps Modem Description

- V.90 uses PCM (pulse coded modulation)
- Bits are sent from the transmitting modem over the digital telephone network to a receiving modem at the telco office.
- Converted to analog voltage levels that are sent over the analog wire to your modem.
56 kbps Modem Description

• Voltages held on the line for 125 microseconds (8000 per second).
• 8 bits per pulse equals 64 kbps
  – North American networks use 7 bits = 56 kbps
• This is the theoretical rate, but is limited by the connection.
V.90 Modem Connection

CellularCrypto.com
4PSK Modulator, 1200 bps

data_rate = 1200 bps

Rounding Function

Phase Table

1200 Hz carrier

Trigonometric Function

cos

Product

psk_out

8000 kHz audio samples

Trigonometric Function1

sin

Product1

1200 Hz carrier
Phase Modulation Over GSM Voice Channel Demonstration
Frequency Modulation Over GSM Voice Channel Demonstration
Technical Details of Proposed GSM Voice Channel Modem and Cryptosystem
Proposed System Block Diagram
Encoder System Diagram

- A/D
- Speech Coder: 16 kHz, 13 bits per sample
- Crypto: 2.4 kbps
- ECC: AES block cypher
- r=1/2 conv. code
- Speech Modem Modulator: 8 kHz, 13 bit samples out

CellularCrypto.com
Decoder System Diagram

- Speech Modem Demodulator
  - Viterbi decoder
- ECC Decoder
- Crypto
  - AES block cypher
- Speech Decoder
- D/A
  - 16 kHz, 13 bits per sample

CellularCrypto.com
Generated speech channel output

Randomly generated "speech" data: 30 frames @ 8000 Hz sampling rate

- Original generated speech
- Output of simulated GSM channel

Amplitude (normalized)

Sample (sampling rate = 8 kHz)
Bit persistence in actual speech data
1000 frames
Speech Modem over GSM Voice Channel Demonstration
Underlying Cryptosystem

AES Block Cipher – Symmetric
- Fixed 128-bit block size
- 256-bit key

Exchanged over modified Diffie-Hellman

Adaptations to allow for frame drops
- Incrementing counter instead of typical block chaining

White Paper to be released during presentation.